# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-173890
(43)Date of publication of application : 13.07.1993

(51)Int.Cl. G06F 12/14
G06K 19/073

(21)Application number : 04-114763 (71)Applicant : GAO GES AUTOM ORG MBH
(22)Date of filing : 07.05.1992 (72)Inventor : WEIKMANN FRANZ

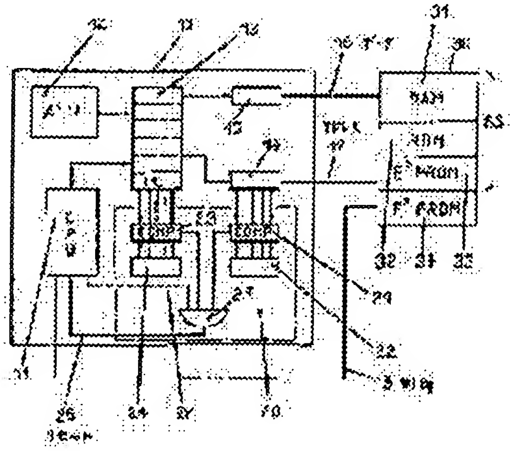
(30)Priority
Priority number : 91 4115152 Priority date : 08.05.1991 Priority country : DE

## (54) DATA PROTECTIVE MICROPROCESSOR CIRCUIT FOR PORTABLE DATA CARRIER

(57)Abstract:

PURPOSE: To inhibit the access to an illegal storing area through the execution of a user program in a data protective microprocessor for portable data carrier.

CONSTITUTION: A comparator 21 compares the content of an address register 14 with that of an auxiliary register 22 and, when the address value in the register 14 is smaller than an address (w) in the register 22, the comparator 21 discriminates that a secondary program is performing access to an illegal storing area and outputs a signal. Another comparator 23 compares the content of a program counter PC with that of the register 24 and, when the content of the counter PC is equal to or larger than the value (w) in the register 24, the comparator 23 discriminates that the secondary program is being executed and outputs a signal. When both comparators 21 and 23 output signals, an AND gate 25 outputs a reset signal to a control unit 11 through a line 26 so as to inhibit the execution of the secondary program.



LEGAL STATUS

[Date of request for examination] 28.04.1999

[Date of sending the examiner's decision of rejection] 08.04.2003

[Kind of final disposal of application other than the

| | |
|---|---|
| examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | 3529800 |
| [Date of registration] | 05.03.2004 |
| [Number of appeal against examiner's decision of rejection] | 2003-12780 |
| [Date of requesting appeal against examiner's decision of rejection] | 07.07.2003 |
| [Date of extinction of right] | |

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] A microprocessor at least A piece and the memory for system actuation, It consists of at least one memory in which a free program is possible according to the individual for every secondary program. In the data protection microprocessor circuit which forbids access to the data or the program memorized in memory First means to supervise the specific effective address, and second means to supervise the specific contents of the microprocessor program counter, The data protection microprocessor circuit characterized by having third means to link the signal from said monitor means and to generate a block signal.
[Claim 2] It is the data protection microprocessor circuit according to claim 1 characterized by preparing the protection network which consists of the second and third means for a start [ said ] in the hard-wired logic on the circuit which has said microprocessor.
[Claim 3] Each of said monitor means consists of an auxiliary register and a comparator, and said auxiliary register is the desired value (setpoints) for the addresses. It is the data protection microprocessor circuit according to claim 1 or 2 characterized by having the program counter reading (program counter readings), and connecting said comparator to the program counter or address register of an auxiliary register and a microprocessor respectively.
[Claim 4] Said link means is a data protection microprocessor circuit according to claim 1 or 2 characterized by being the AND gate connected to the outgoing end of said comparator.
[Claim 5] Said desired value is the data protection microprocessor circuit of claim 1-4 characterized by being held in the field of the operating system which cannot be accessed and being loaded to said auxiliary register in process of initial setting of said microprocessor given in any 1 term.
[Claim 6] Said block signal from said link means is the interruption input (interrupt input) of said microprocessor. Data protection microprocessor circuit of claim 1-5 characterized by connecting with an edge given in any 1 term.
[Claim 7] Said block signal from said link means is the data protection microprocessor circuit of claim 1-6 characterized by connecting with the reset input edge of said microprocessor given in any 1 term.
[Claim 8] Said protection network is a data protection microprocessor circuit according to claim 1 or 2 characterized by being the second microprocessor called a protection processor.
[Claim 9] Said microprocessor called said protection processor and the activity processor which performs said secondary program control is the data protection microprocessor circuit of claim 1-8 characterized by being prepared on the same integrated circuit given in any 1 term.
[Claim 10] Said protection processor is the data protection microprocessor circuit of claim 1-9 characterized by operating with a clock frequency higher than said activity processor given in any 1 term.
[Claim 11] It connects with limit memory and said protection processors are the possible contents (possible contents) of the program counter of an executive address and said activity processor in the limit memory concerned. It is the data protection microprocessor circuit of claim 1-10 which the related limiting value is memorized and is characterized by the ability of said activity processor not to access at

the memory concerned given in any 1 term.

[Claim 12] A microprocessor at least A piece and the memory for operating systems, In the data protection microprocessor circuit which forbids access to the data or the program which is equipped with at least one memory in which a free program is possible according to the individual the whole secondary program, and was memorized in memory The one most significant is removed at least. Two or more freely programmable memory storage with the same address space, The data protection microprocessor circuit characterized by outputting a block signal if it consists of auxiliary registers with which the specific most significant corresponding to memory storage is loaded and change arises by the contents of said auxiliary register before addressing memory storage.

[Claim 13] The data protection microprocessor circuit according to claim 12 characterized by loading the most significant of said address bus to an unit or two auxiliary registers which were connected to the comparator.

[Claim 14] The data protection microprocessor circuit according to claim 1 to 13 characterized by processing reading / write-in signal from said microprocessor in said protection network, and blocking reading or writing alternatively.

---

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the data protection microprocessor which forbids access to the data or the program memorized especially in memory about a data protection microprocessor circuit.
[0002]
[Description of the Prior Art] The microprocessor circuit of the above-mentioned type is widely used for the so-called chip card equipped with integrated circuits, such as an ID card, a credit card, and a transcript card (posting card). payment module (payment modules) which communicates with the above-mentioned card through an interface with these suitable microprocessor circuits etc. -- it is possible to use it.
[0003] In order to help an understanding of this invention, the example which used the microprocessor circuit for the card is explained.
[0004] The card equipped with the microprocessor is German patent DE-OS. 27 In 38113, it is indicated for the first time. The effectiveness that the use range of the owner of a card spreads as one of the advantages of such a card is mentioned. It becomes possible to perform data processing broadly for card itself with the microprocessor laid under the interior of an integrated circuit or a card, and the storage means corresponding to it. On the other hand, with the card to which the magnetic strip was attached, all data processing functions needed to be performed externally.
[0005] For this reason, a card manufacturer can equip said microprocessor with the resident operating system which performs basic functions, such as procedure which compares the code remembered to be the code inputted from the outside. Said store incidental to said microprocessor has memorized said not only operating system but specific application, the parameter with which protection indispensable to a security check etc. and perfect is demanded.
[0006] It is made to start with the operating system equipped with the correspondence program, and specific INTAFESU is defined, and if the memory or memory storage for the so-called secondary program is secured, the application range of a card will spread further. For this reason, a card manufacturer is a user (card-issuing organization), i.e., a card issuing organization, about the memory or the storage region for programming an original secondary program. It provides. The organization concerned can specify a specific operation in the secondary program only relevant to a specific organization unrelated to an operating system.
[0007] As for programming a secondary program original in the chip card by which preforming was carried out depending on the case, not only one organization but two or more different organizations may program an original program respectively.
[0008] Anyway, he needs to understand that the data about the protection which is a part of said operating system or each second program are protected from unauthorized access.
[0009]
[Problem(s) to be Solved by the Invention] Thus, the simple thing of the configuration of a circuit in

which a secondary program is made to access only memory storage to which access was permitted clearly is desirable.

[0010] Even if this invention is made in view of the technical problem which such a conventional technique has and the purpose performs a user program, it is in offering the protection network which can prevent access to an illegal storage region (illegal memory areas) with a simple configuration.

[0011]

[Means for Solving the Problem] in order to attain the above-mentioned purpose -- the first operative condition of this invention -- the data protection circuit which starts like is characterized by consisting of the first means to supervise the specific selected address, the second means to supervise a microprocessor program counter, and the third means to link the signal from said monitor means and to generate a block signal.

[0012] Moreover, the data protection circuit concerning the second embodiment of this invention is characterized by consisting of an activity microprocessor which performs a secondary program, and a protection processor which performs the monitor of the activity processor concerned.

[0013] Furthermore, the data protection circuit concerning the third embodiment of this invention is completely equipped with the same address space except for at least one most significant, and is freely characterized by having the programmable storage region in two or more pans.

[0014]

[Function and Effect] the configurations with the above data protection circuit of this invention -- carrying out -- **** -- said first operative condition -- in the data protection circuit which starts like, since the readings of a program counter are supervised, the load program by which current activation of said protection network is carried out can always supervise which it is Moreover, when the address called to the specific program under activation is being supervised to coincidence, it can be easily coped with by outputting a reset signal to said microprocessor through a coupled circuit as opposed to illegal access to a storage region.

[0015] From an actual microprocessor, said protection network has a microprocessor, although it dissociates (taking up). It is desirable although prepared on an integrated circuit. Specific program counter readings and the desired value corresponding to the address are set up beforehand, and a desired storage region can be permitted to a specific user, can be made into disapproval, or can be defined. When reading or the writing of a specific storage region is blocked alternatively, reading / write-in signal from said microprocessor will be processed also in said protection network with a natural thing.

[0016] Moreover, in the data protection circuit of this invention concerning said second embodiment, since said activity processor is always under control of a protection processor, it operates for every reset, and it performs continuing initial setting. when it is detected by said protection processor that said activity processor which is executing the specific secondary program has accessed the illegal storage region, as for the protection processor concerned, the mask of the activity processor is not carried out -- interrupting -- an input edge -- or a block signal is outputted to a reset input edge.

[0017] Since said protection processor is supervising the whole of each step of said activity processor, it operates with a clock frequency higher than said activity processor to a desirable thing.

[0018] When two or more secondary programs are memorized in the memory corresponding to said activity processor, it is necessary to forbid said not only operating system but access to other secondary programs. For this reason, the required reference value is memorized as limiting value in the limit memory corresponding to said protection processor. This memory supports said protection processor and contains the limiting value about the possible contents of the address under monitor, or the program counter of said activity memory. Access of said activity processor to such memory storage is forbidden.

[0019] When unauthorized access to a storage region is performed, only a series of instructions which can be translated are executed and secondary program execution is prevented. Next, an instruction of the secondary program concerned is executed based on control of an operating system, and access is performed only in the field in which access is permitted. Thus, the program counter of said microprocessor is not controlled by the secondary program.

[0020] Furthermore, according to the third embodiment of this invention, before addressing a storage region, the specific most significant corresponding to the storage region concerned is loaded to an auxiliary register. A block signal is outputted whenever an auxiliary register's contents of data change. Said microprocessor defines a specific user for every load actuation of said auxiliary register. When this user accesses an illegal storage region and said auxiliary register's contents change according to this, said protection network which is supervising the auxiliary register's contents generates a block signal.

[0021]

[Example] Hereafter, the suitable example of the data protection microprocessor concerning this invention is explained, using a drawing.

[0022] Drawing 1 shows the structure of data carriers, such as the credit card 1 which consisted of integrated circuits 5 which are equipped with the vision data area 2, the name stripe 3, and a terminal 6, and are embedded. Here, the connector contact 6 is arranged at two trains. Since the basic structure of such a card is fully known, the detailed explanation is omitted. Furthermore, the use gestalt and data-processing method of such a credit card are also common knowledge. Exchange of the terminal of an automatic cash-drawer machine etc. and data is performed through the connector contact 6. In the integrated circuit of the credit card concerned, a protection routine required to give the user of a card rating etc. is performed.

[0023] Drawing 2 shows the first example of the integrated circuit in the condition of having been built in the credit card. The microprocessor 10 consists of the control unit 11 connected to the memory array 30 through the control line 18, the logic unit (ALU) 12, a register file 13, an address register 14, and a data register 15. The register of said register file 13 functions as a program counter, and it specifies which address the contents of this counter access, in order to take out an instruction of the secondary program memorized by the memory array 30. That is, a data item is read from one address of said memory with this instruction. For this reason, the address for specifying which address is accessed at the time of access to a next storage region is stored in the address register 14. This address is outputted to a memory array 30 through a bus 17. The reading data from the writing or memory 30 to said memory 30 are supplied to a data register 15 through a data bus 16, and are further sent out from a data register 15 even to the register of a register file 13.

[0024] E2 PROMs33 are consisted of by the memory array 30 with reading / write-in memory (RAM) 31, and read only memory (ROM) 32 as shown in drawing. These storage regions 31, 32, and 33 are included in the operating system (BS), and the protection associated data with which perfect secrecy is demanded is contained in these some operating systems. the simple operative condition shown in drawing 2 R> 2 -- the operating system (BS) using the secondary program in order to protect such data like -- the user access to all the storage regions 31, 32, and 33 is prevented.

[0025] A user's access is possible, and for this reason, protection-related data need to use the protection network 20 explained below for the remaining address in an operating system to be protected, when a manufacturer prepares the field which is not stored in an operating system. As a user can access the field of said operating system by the secondary program, in order to compare a routine, i.e., the inputted consecutive numbers, and the consecutive numbers stored by the protection state in the operating system, since a user can use said secondary program, the writing to the secondary program by the user becomes easy.

[0026] Moreover, the memory array 30 is equipped with the storage region 34 for a secondary program. A different organization from the manufacturer of a card can load this secondary program. For this reason, the secondary program which the user loaded occupies the location from w of a storage region to x, and, on the other hand, as for said operating system, the locations from 0 to w-1 of a storage region will be occupied.

[0027] In order to check whether the drawer of the service, i.e., deposit, which the owner of a card demanded etc. can permit said secondary program according to a cardholder's deposit balance, it consists of a routine and data specially. After the owner of a card inserts a card in a machine, exchange of data is performed between machines and microprocessors 10 concerned. If a specific routine is started and performed with an operating system, the program counter PC within the secondary program 13 stored in the storage region 34, for example, the register file set as Address w, will perform an operation further. Consequently, an instruction of the secondary program stored in the first storage location of a storage region 34 is called.

[0028] In order to prevent a secondary program accessing storage regions 31 and 32 and the address in 33, the protection network 20 concerning this invention is arranged. This protection network is established also in the microprocessor 10 and the memory array 30 again. All these components are constituted as a one chip integrated circuit.

[0029] The protection network 20 consists of output Rhine 26 which connects the first comparator 21, the first auxiliary register (HRI) 22, the second comparator 23, the second auxiliary register (HRII) 24, the AND gate 25, this AND gate 25, and the control circuit 11 of a microprocessor 10.

[0030] Said comparator 21 compares the contents of an address register 14 and the auxiliary register 22, and the another side comparator 23 compares the contents of a program counter and the auxiliary register 24.

[0031] A manufacturer can program said auxiliary registers' 22 and 24 contents beforehand within hard-wired logic. Furthermore, these contents can also be loaded to an auxiliary register from the memory of a protection state using an operating system in process of initial setting of a microprocessor.

[0032] The address w which starts the secondary program in a storage region 34 is loaded to the auxiliary register 22. The value w is similarly memorized by the auxiliary register 24. When the address stored in said address register 14 is smaller than the address w stored in the auxiliary register 22, said comparator 21 outputs a signal (that is, when the secondary program has accessed the illegal storage locations from 0 to w-1). Moreover, it is equal to the value w with which the contents of the program counter PC of a register file 13 are stored in the auxiliary register 24, or when it is more than it, a comparator 23 outputs a signal. In the case of the latter, the secondary program will be performed.

[0033] When the both sides of comparators 21 and 23 output a signal, the illegal address which a secondary program is performing and is out of the address space of the secondary program concerned will be accessed. At this time, the AND gate 25 outputs a reset signal etc. to a control unit 11 through Rhine 26, and subsequent secondary program execution is prevented.

[0034] In order to prevent reading or write-in actuation alternatively, reading / write-in signal from a microprocessor are processed even in a protection network 20 (Rhine 27 reference).

[0035] When the storage region for a secondary program which a different user loads as a mode of others of the example shown in drawing 2 exists further, the comparator corresponding to an auxiliary register can be added further.

[0036] The second example of this invention is illustrated by drawing 3 . The activity processor 110 corresponding to a memory array (PROM) 130 of the microprocessor 10 and function corresponding to a memory array 30 of drawing 2 is substantially the same.

[0037] Here, said protection network is the secondary processor 120, i.e., the protection processor equipped with the memory array 150 of a proper.

[0038] The operation clock signal C1 determines a speed of the protection processor 120 of operation. The frequency of said timing signal will be carried out by the frequency divider 140 n dividing, and the activity processor 110 into which the output signal from said frequency divider 140 is inputted will operate at the rate of only 1/n of the protection processor 120.

[0039] Said protection processor's 120 detection of access of the secondary program to an illegal storage region forms in it the control unit 121 which outputs a reset signal to said activity processor 110. In order to perform such detection, the monitor of the address line 117 and control line 118 which connect the activity processor 110 and a memory array 130 is performed, and the program counter (PC) of said activity processor is supervised further. The data on an address bus 117 and the both sides of the contents of said program counter PC are compared with specific limiting value for every secondary program.

[0040] Two or more storage regions User I, User II, and for **(ed) different users are established in the memory array 130 for said activity processor 110. As mentioned above, a different organization from a card manufacturer loads these secondary programs uniquely. As for the storage regions 134, 135, and 136 of a memory array 130, it is desirable to constitute from a nonvolatile memory (for example, E2 PROM) etc.

[0041] When the activity processor 110 performs after initialization a specific secondary program, for example, the program stored in User's I storage region 134, the protection processor 120 compares the correspondence limiting value for the users concerned for a specific address signal and a program counter. Such limiting value is stored in the memory array 150 as some operating systems of the protection processor 120. When performing User's I secondary program etc., the contents of the program counter PC will cover only the value of the specific range. Moreover, the address on an address bus 117 must correspond only with the value of this range. When a difference is between the address and a value, said processor 120 outputs a reset signal to the activity processor 110, and prevents secondary program execution.

[0042] The third example of this invention is shown in drawing 4 , and according to this example, the operating system memory 231 corresponding to a microprocessor 210 is separated and arranged in storage regions 234, 235, and 236. These storage regions perform ejection for the secondary program for three different users. It is connected with the address bus and the control bus between a microprocessor 210 and memory 234, 235, and 236, i.e., storage regions.

[0043] The address space for accessing to the aforementioned (PROM) storage regions 234, 235, and 236 consists of 16 bits, and the most significant 2 bits specify whether current access is made in which memory or storage region. As the whole, four memory or a storage region (00, 01, 10, 11) can be chosen by said most significant 2 bits.

[0044] The value which consists of 2 bits in the case of this example is inputted into the first auxiliary register 222 (HRI) in a protection network 220 from the operating system controlled by the variable of a user proper before performing a secondary program. For example, when it has the address with which the secondary program in memory 234 is performed, and this memory becomes said top location of 2 bits from the combination of the bit of "01", value"01" is memorized in a memory register 222.

[0045] At the time of the beginning which performed the secondary program, i.e., first-address assignment, the two top locations of an address register are loaded in the second auxiliary register (HRII) 223 through an address bus, and the comparator 221 which compares the contents of the auxiliary registers 222 and 223 is started with the correspondence control signal from a microprocessor. When the contents of the auxiliary program 222 are in agreement with the contents of the auxiliary register 223, the second program will operate only in a corresponding address tooth space (storage region 234). When the different address is accessed, the location of the two most significants of said address signal changes, and the contents of said auxiliary register 223 also change. Such change is detected by the comparator and a reset signal is outputted to a microprocessor 210 through Rhine 226.

[Translation done.]